Smart Metering Implementation Programme

SMKI and Repository Testing Approach

Version: 3.2
Date: 20/01/2016

Document History

Version	Date	**Comment**	Author
0.1	06/10/14	Initial draft for DCC review	DCC
0.2	31/10/14	Updated following internal review	DCC
0.3	03/11/14	Updated following DCC review	DCC
0.4	19/11/14	Updated following DCC review	DCC
1.0	28/11/14	Published as Working Document	DCC
1.0.1 – 1.0.5	13/03/15	Updated following comments received on Working Document and DCC review	DCC
1.1	05/03/15	Reviewed by DCC, DCC Service Providers and DECC	DCC
2.0	13/03/14	Up-issued and published for consultation	DCC
2.1	22/04/15	Updated following consultation	DCC
2.2	30/04/15	Updated following review by Testing Advisory Group, DECC and DCC	DCC
2.3	01/05/15	Submitted to SMKI PMA and SEC Panel for approval	DCC
3.0	29/05/15	Up-issued for publication	DCC
3.1	11/01/16	Updated to reflect phased implementation	DCC
3.2	20/1/16	Updated following DCC and DCC review comments prior to consultation	DCC

References

Abbreviation	Title & Originator's Reference	Source	Release Date	Version
SEC	Smart Energy Code	DECC	21 Oct 15	SEC 4.6
CTSD	Common Test Scenarios Document	DCC	28 Aug 15	Baselined V1.0
JTS	Joint Test Strategy	DCC	9 Apr 15	3.5
SIT Approach	Systems Integration Test Approach	DCC	21 Sep 15	4.0
SMETS2	Smart Metering Equipment Technical Specifications	DECC	3 Dec 15	1.59
SRTSD	SMKI and Repository Tests Scenarios Document	DCC	N/A	SEC Appendix K
DCC SP Contract	DCC Service Provider Contracts	DECC / DCC	23 Sep 13	v.1

Glossary of Terms

Abbreviation	Title & Originator's Reference
ARL	Authority Revocation List
ARO	Authorised Responsible Officer
The Authority	The Gas and Electricity Markets Authority as established under section 1 of the Utilities Act 2000.
CRL	Certificate Revocation List
CSP	Communications Service Provider
DCC	Smart DCC + all Service Providers
DSP	Data Service Provider
FIPS Token	Federal Information Processing Standard Token
IKI	Infrastructure Key Infrastructure
IRB	Issue Resolution Board
KAK	Key Agreement Key
MAC	Message Authentication Code
PIT	Pre-Integration Testing
Panel	The Smart Energy Code Panel
Parties	A SEC Party - a person/entity that has agreed to be bound by this Code (either pursuant to the Framework Agreement or an Accession Agreement)
PKI	Public Key Infrastructure
PPMID	Prepayment Interface Device
SMKI RAPP	SMKI Registration Authority Policies and Procedures
RDP	Registration Data Provider
RTM	Requirements Traceability Matrix
SEC	Smart Energy Code
SFTP	Secure File Transfer Protocol
SIT	Systems Integration Testing
Smart DCC	Data Communications Company
SMKI	Smart Metering Key Infrastructure
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SMIP	Smart Metering Implementation Programme
SP	Service Provider
SP UAT	Service Provider User Acceptance Testing
SREPT	SMKI and Repository Entry Process Testing (part of the User Entry Process)
SRTSD	SMKI and Repository Tests Scenarios Document
SRT	Smart Metering Key Infrastructure and Repository Testing
SSD	SEC Subsidiary Document
TSP	Trusted Service Provider (the Service Provider delivering the SMKI Service)
UIT	User Integration Testing

Definitions

Term	Definition	Source
Batched Certificate Signing Request	A single communication containing Certificate Signing Requests for the Issue of more than one but no more than 50,000 Device Certificates.	SEC
Contingency Key Pair	a Key Pair established by the DCC for the purposes of the replacement of all Certificates including Root OCA Certificates on Devices after a Relevant Private Key has been Compromised	SEC
Contingency Private Key	the Private Key which is part of that Key Pair	SEC
Contingency Public Key	the Public Key which is part of that Key Pair and which is stored in the WrappedApexContingencyKey field of the Root OCA Certificate (being the field identified as such in the Root OCA Certificate Profile at Annex B of the Organisation Certificate Policy)	SEC
Device	Means one of the following individual Devices: (a) an Electricity Smart Meter; (b) a Gas Smart Meter; (c) a Communications Hub Function; (d) a Gas Proxy Function; (e) a Pre-Payment Interface; (f) an Auxiliary Load Control; and (g) any Type 2 Device.	SEC
Device Certification Authority (DCA)	Means the DCC acting in the capacity and exercising the functions of one or more of: a) The Root DCA b) The Issuing DCA	SEC
Entry Criteria	The criteria that must be satisfied before testing can commence	SEC
Exit Criteria	The criteria that must be satisfied before testing can be considered complete	SEC
Good Industry Practice	Means exercising that degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced provider of services	UK Govt Services & Goods contract
IKI Certification Authority (ICA)	Means the DCC, acting in the capacity and exercising the functions of one or more of: (a) The Root ICA (b) The Issuing ICA	IKI Cert' Policy
Install & Commission	The process of installing and commissioning Smart Metering equipment between Service Users, metering equipment and the DCC Service.	CTSD
Issuing Device Certification Authority (or Issuing DCA)	Means the DCC exercising the function of Issuing Device Certificates to Eligible Subscribers and of storing and managing the Private Keys associated with that function	SEC
Issuing OCA	Means the DCC exercising the function of Issuing Organisation Certificates to Eligible Subscribers and of storing and managing the Private Keys associated with that function	SEC
Motorway	The components of the DSP solution that process and carry communications between Service Users and Smart Meters i.e. Service Requests. The components are: a) DCC User Message Gateway b) Request Management c) Data Communication component	JTS

Term	Definition	Source
Organisation Certification Authority	Means the DCC acting in the capacity and exercising the functions of one or more of: d) The Root OCA e) The Issuing OCA	SEC
(SMKI) RAPP	SMKI Registration Authority Policies and Procedures	SEC
Recovery Key Pair	a Key Pair established by the DCC for the purposes of the replacement of Organisation Certificates on Devices after a Relevant Private Key has been Compromised	SEC
Recovery Private Key	the Private Key which is part of that Key Pair	SEC
Recovery Certificate	an Organisation Certificate Issued by the OCA and containing the Public Key which is part of that Key Pair	SEC
(SMKI) Registration Authority	Means the DCC exercising the function of receiving and processing Certificate Signing Requests made in accordance with the SMKI RAPP.	SEC
Regression Testing	Testing to ensure that existing functionality of a system is not affected by the addition of new and modified functionality (or any other change to any related part of any System) introduced at any point in the Service Period (and Regression Test shall be construed accordingly)	JTS
Relevant Private Key	a Private Key which is associated with a Public Key contained in: (i) any Organisation Certificate or OCA Certificate that is held on a Device comprising part of an Enrolled Smart Metering System; or (ii) any OCA Certificate that was used as part of the process of Issuing any such Organisation Certificate or OCA Certificate	SEC
Requirements Traceability Matrix	A list of defined requirements that provides traceability, in a format agreed between the DCC and Service Providers, to design artefacts and test scripts for the purposes of assurance/audit and test coverage	DCC SP Contract
Smart Metering Key Infrastructure (or SMKI)	The public key infrastructure established by DCC for the purpose, among other things, of providing secure communications between Devices and Users	DECC conclusions on amended SEC text, March 2015
SMKI Compliance Policy	The Policy as defined in Appendix C of SEC3	SEC
Test Completion Certificate	A Certificate issued by the DCC to a User when the User successfully completes testing.	CTSD
Test Data	The data constructed for the purposes of undertaking Tests.	CTSD
Test Data Plan	The document that sets out: the size and type/format of data, who is responsible for providing the data; and when the data is required to be available to support test activities in a Test Plan.	CTSD
Test Exit Report	A report that sets out the results of testing during the Test Stage and demonstrates the manner in which the Exit Criteria have been attained.	CTSD
Test Management Tool	A tool that has the ability to log and track Testing Issues, store Test Scripts, map Test Scripts to requirements, enable test execution and track test progress.	CTSD
Test Plan	A document describing the scope, approach, resources and schedule of intended test activities within a Test Stage that will	CTSD

Term	Definition	Source
	be produced.	
Test Result	The consequence/outcome of the execution of a test script.	CTSD
Test Readiness Report	A report that when completed provides the capability to assess the status of test preparation and determine the readiness to proceed into test execution.	CTSD
Test Schedule	A list of test process activities, tasks or events identifying their intended start and finish dates and/or times and interdependencies.	CTSD
Test Script	A document specifying a sequence of actions for the execution of a test.	CTSD
Test Stage	A group of test activities that are organised and managed together	CTSD
Testing Participant	Means, in respect of each Testing Service, the persons (whether or not they are Parties) who are entitled to undertake such tests, as described in Section H14 (Testing Services), together with any other persons identified as such in Section T (Testing During Transition).	SEC
Type 1 Device	A Device, other than GSME, ESME, Communications Hub Function or Gas Proxy Function, that stores and uses the Security Credentials of other Devices for the purposes of communicating with them via its HAN Interface.	SMETS
User Systems	means any Systems (excluding any Devices) which are operated by or on behalf of a User and used in whole or in part for: (a) constructing Service Requests; (b) sending Service Requests over the DCC User Interface; (c) receiving, sending, storing, using or otherwise carrying out any processing in respect of any Pre-Command or Signed Pre-Command; (d) receiving Service Responses or Alerts over the DCC User Interface; (e) generating Data for communication by means of the Self-Service Interface, or receiving Data that are communicated by means of the Self-Service Interface; (f) generating Data for communication to the OCA or DCA, or receiving Data from the OCA or DCA (including any Systems which store or use Secret Key Material for such purposes); and (g) generating Data for the purposes of lodging in the SMKI Repository, or retrieving Data from the SMKI Repository.	SEC

Contents

1 Introduction

1.1 Background

The Government's vision for every home in Great Britain is to have smart energy meters by 2020. To achieve this vision, the Department of Energy and Climate Change (DECC) has created the Smart Metering Implementation Programme (SMIP). The SMIP is a customer-focused, energy supplier-led approach to the roll-out of an estimated 53 million smart electricity and gas meters to homes and small businesses across Great Britain.

The role of the Data and Communications Company (DCC) is to provide the shared infrastructure necessary for smart meters to operate consistently for all consumers, regardless of their energy supplier. This infrastructure will offer new opportunities for consumers to receive energy services and to reduce their energy usage, as well as provide smart metering data to network operators in support of smart grids.

The DCC has procured a Smart Metering Key Infrastructure (SMKI) service, which provides the means by which Smart Energy Code (SEC) Parties establish trust across the DCC network and one of the primary mechanisms by which communications between Users and Devices are secured. SMKI Certificates secure messages between SEC Parties and Devices by providing assurance of the identity of each entity. They are also used to sign DCC User Interface (DUIS) commands sent to DCC. An overview of the scope of the SMKI service is provided in section 2 of this document.

To gain access to SMKI Interfaces, credentials are issued to Authorised Responsible Officers to authenticate to those SMKI Interfaces. These credentials are issued under the Infrastructure Key Infrastructure (IKI) Certificate Policy. The credentials used to authenticate the interfaces to the SMKI Service and SMKI Repository are shown in figures 2 and 3 in section 5 of this document.

SMKI and Repository Testing (SRT) tests the capability of the DCC and the component parts of the DCC Systems to interoperate with the Systems of Parties to the extent necessary for the SMKI Services and the SMKI Repository Service.

This document is required by Section T5.5 of the SEC. The purpose of this document is to set out how SRT is performed such that the DCC can demonstrate that it is capable of complying with its obligations under Section L of the SEC. The purpose of the document is set out in further detail in section 3.2 of this document.

1.2 Reviews, Approvals and Appeals

As required by Section T5.7 of the SEC, the DCC will consult on the SRT Approach Document. The document, having been revised to accommodate consultation responses, will be presented to the Testing Advisory Group (TAG) for review and then to the SEC Panel for approval, along with the responses from consultation. It will be published on the DCC website, www.smartdcc.co.uk, as directed by the Secretary of State.

The document can be rejected by the SEC Panel prior to approval and the decision of the SEC Panel (to either approve or reject the document) can be appealed. The SEC[1] sets out the process that will be followed by the DCC in such an event.

[1] Sections T5.8 to T5.10 apply

2 Scope

2.1 Overview

SMKI and Repository Testing will test the capability of the DCC and the component parts of the DCC Systems to interoperate with the Systems of Parties, and RDPs to the extent necessary for the SMKI Services and the SMKI Repository Service. The diagram below gives an overview of the SMKI Solution.

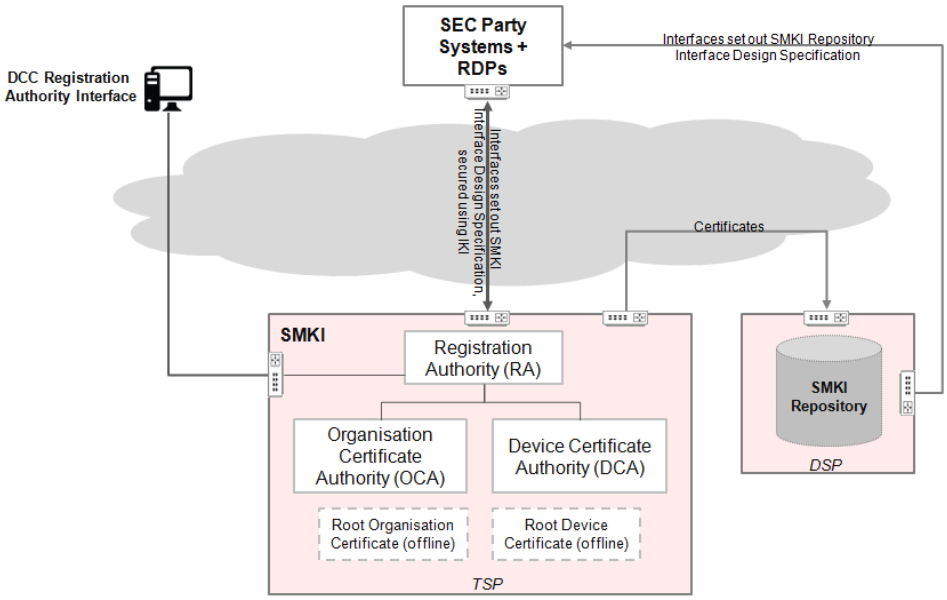


Figure 1 - SMKI Overview

Section 5, Scope of Testing, sets out a more detailed view of the SMKI Service and SMKI Repository Service, along with detail of the credentials used to authenticate to the SMKI Repository and SMKI Repository Service. SRT will test the SMKI Service, SMKI Repository Service and the interfaces to each.

2.2 The SMKI Service

The SMKI Service encompasses the activities that are undertaken by the DCC in its capacity as the Device Certification Authority (DCA), the Organisation Certification Authority (OCA) and the Infrastructure Key Infrastructure (IKI) Certification Authority, in each case in accordance with the applicable requirements of the Smart Energy Code.

2.3 The SMKI Repository Service

The SMKI Repository Service encompasses the activities undertaken by the DCC to establish, operate, maintain and make available the SMKI Repository.

The SMKI Repository is a System for storing and making available copies of SMKI & IKI artefacts as detailed in the SEC L5.1.

2.4 File Signing

A Private Key corresponding with an IKI File Signing Certificate is used for signing communications via the DCC Service Desk (for the purposes of Threshold Anomaly Detection and Certified Product List). This is delivered and tested in SRT2a ahead of testing the delivery of these files during SIT for R1.2.

IKI File Signing Certificates are also used for SMKI Recovery File Signing, which is delivered and tested in SRT3.

Registration Data Providers will use the Private Key associated with their SMKI Organisation Certificate to sign Registration Data files.

3 Objectives

3.1 SRT Objective

The objective of SMKI and Repository Testing (SRT) is to demonstrate that the DCC and the DCC Systems interoperate with each other and with Systems of Parties, and RDPs to the extent necessary in order that the DCC is capable of complying with its obligations within the Smart Energy Code, at the levels of activity reasonably anticipated during the period of Interface Testing and set out in the SEC, Section L - Smart Metering Key Infrastructure.

SRT is a discrete test stream within the testing lifecycle:

- **Part 1 SRT (DCC Testing conducted in isolation from other SMIP Test Phases)**: to test the SMKI test Service and test SMKI Repository in isolation (along with testing the interfaces), and is limited to the issuance of Test Certificates including the lodging of Test Certificates into the test SMKI Repository. No Parties will participate in this testing, with the DCC performing these tests. Part 1 is subdivided into Part 1a, which tests the SMKI interfaces available via the DCC Gateway Connection; and Part 1b, which tests the interfaces available via the internet portal.
- **Part 2 SRT (DCC Testing conducted during SIT)**: Part 2a, which validates the integration of the SMKI and Repository Service with the wider DCC systems, where particular focus will be given to the interfaces between the test SMKI Repository and the DSP; and Part 2b to test the SMKI Recovery functionality involving the Apex Contingency Key. No Parties will participate in this testing, with the DCC performing these tests.
- **Part 3 SRT (Remaining SMKI Recovery functionality)**: Part 3 tests the remaining SMKI recovery functionality involving the Recovery Key. This testing will be defined in the SMKI Recovery Procedure, which is an enduring SEC Subsidiary Document.
- **SMKI & Repository Entry Process Testing (SREPT)**[2] against the SMKI test Service. Parties, RDPs and non-Users must successfully complete the SREPT on the SMKI test Service (incorporating test SMKI Repository) before Live SMKI Certificates can be obtained. This testing may be undertaken after Part 1a or Part 1b SRT has been completed, as required..

3.2 SRT Approach Purpose

The purpose of the SRT Approach Document is to explain how SRT is to be undertaken, including obligations of the DCC and each other Party / RDP and sets out:

- the reasonable entry criteria to be satisfied by the DCC with respect to the commencement of SRT;

[2] SMKI and Repository Entry Process Tests are detailed in the SMKI & Repository Tests Scenarios Document (SRTSD). As a consequence, this SRT Approach will not provide any detailed information for the initiation, execution and completion this specific element of testing.

- the entry criteria[3] to be met by each Party prior to its commencing the SMKI and Repository Entry Process Tests (which criteria shall be consistent with the relevant requirements of Section H14 (Testing Services), subject only to amendments reasonably required for the purposes of SMKI and Repository Testing);
- the manner in which SMKI and Repository Testing is to be undertaken, including the respective obligations of the DCC and each other Party;
- a reasonable timetable for undertaking and completing SRT;
- the frequency and content of progress reports concerning SRT to be provided by the DCC to the Panel;
- the process by which the DCC will facilitate Parties undertaking and completing the SMKI and Repository Entry Process Tests[4];
- a Good Industry Practice methodology for determining whether or not the SRT Objective has been achieved, including details of the exit criteria to be achieved and the level of assurance that will be delivered by achievement of those exit criteria; and
- how the DCC will report to the Panel where the DCC considers that the exit criteria have been achieved (providing evidence of such achievement), having consulted with the Parties who have participated in SMKI and Repository Testing

3.3 SRT timetable

The plan below illustrates the dependencies between different test activities in order to test the SMKI and Repository systems. The key dependencies are that the SMKI Test Service and Test SMKI Repository are tested individually ahead of Part 1 SRT and that Part 1 SRT completes ahead of SREPT (specifically that Part 1a completes before SREPT involving the DCC Gateway Connection and that Part 1b completes before SREPT involving SMKI via the Internet Portal).

The DCC will publish the start dates Part 1 SRT, Part 2 SRT and SREPT, providing at least 3 months' notice to Parties of the date on which SRT is to commence, or such shorter period as the Secretary of State may direct.

Comment [PJST1]: Note to consultation respondents. This table has been deleted – but is displayed as a tracked change.

[3] These entry criteria are set out in the SMKI & Repository Test Scenarios Document.

[4] This support provided by DCC is set out in section 7.6 and is set out in further detail in the SMKI & Repository Test Scenarios Document.

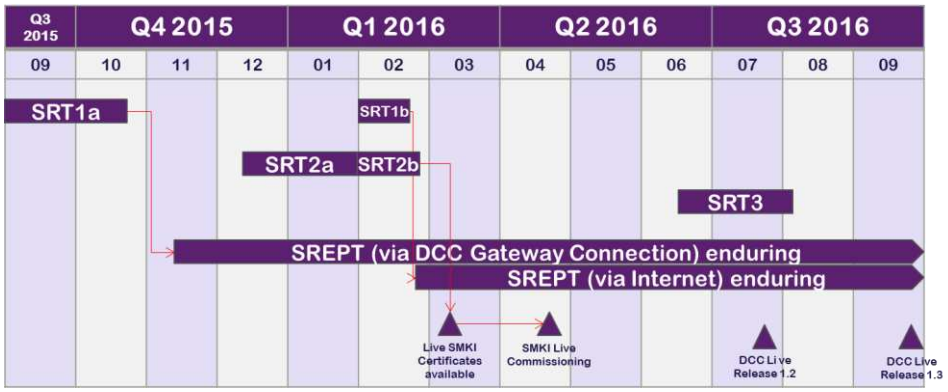


Figure 1 – SMIP Program incorporating SMKI and Repository Testing

'Live SMKI Certificates Available' will support the provision of the SMKI Certificates required during the Device manufacturing process and is shown ahead of 'DCC Live' to facilitate the availability of Devices for live. The focus of Part 1 and Part 2b SRT is to test the functionality required for these processes.

SREPT via DCC Gateway Connection, and via the Internet Portal will commence after the successful completion of Part 1a SRT and Part 1b SRT respectively.

Part 2a SRT will be executed during the Systems Integration Test Phase. This testing will run in parallel with Part 1 SRT and SREPT. The DCC will ensure that Part 2a SRT is managed accordingly to minimise the risks associated with parallel test activities through management of resources and detailed ordering and scheduling of testing activities.

Part 3 SRT will test SMKI Recovery functionality, excluding functionality involving the Apex Contingency Key which will already have been tested in Part 2b. This testing will be defined in the SMKI Recovery Procedures SEC Subsidiary Document (SSD).

3.4 Testing Completed in other Test Stages

Reliance is placed on the testing that is performed on individual components of the solution during Pre-Integration Testing. The functional elements that are tested during Pre-Integration Testing and are not impacted by integration with other systems are not required to be retested during SMKI and Repository Testing.

4 SRT Entry & Exit Criteria

4.1 Part 1 SRT Entry Criteria

The DCC will ensure that the following entry criteria are met by the DSP and TSP for each of Part 1a and Part 1b (referred to as Part 1x, below):

- exit criteria for TSP Pre-Integration Testing successfully met;
- a successful security assessment conducted, likely to include a penetration test that displays no high severity vulnerabilities, which is validated by the DCC prior to integrating the SMKI test Service with the test SMKI Repository;
- DSP test SMKI Repository built, and exit criteria for Pre-Integration Testing of the Repository in isolation successfully met;
- test environments are available;
- Part 1x SRT Test Plan approved by the DCC;
- Adequate resources are available to support the testing;
- Part 1x SRT Test Specifications prepared; and
- a Requirements Traceability Matrix (DSP's and TSP's own RTMs per solution design) produced, which will be consolidated and extended to cover the scope of SRTA, per section 5.9, and approved by the DCC.

4.2 Part 1 SRT Exit Criteria

The DCC will ensure that following exit criteria are met by the DSP and TSP before each of Part 1a and Part 1b SRT can complete:

- 100% of planned tests run, or any exceptions documented and agreed with the DCC;
- at least 85% of planned tests passed, or any exceptions documented and agreed with the DCC;
- the level of defects is within the following thresholds per Service Provider, or any exceptions are documented and agreed with the DCC:
  - 0 Severity 1s (see Appendix A for Severity definitions)
  - 0 Severity 2s
  - 15 Severity 3s
  - 30 Severity 4s
  - 60 Severity 5s;
- the Test Completion Report has been issued in accordance with section 6.2;
- where appropriate, a Work-Off Plan has been produced and agreed by the DCC;

- all test results have been documented and evidence captured;
- a complete set of test issue logs produced

Details of Testing Issues outstanding and recorded on the Work-Off Plan that have the potential to impact Testing Participants undertaking SREPT will be made available to Testing Participants.

The DCC may take advice from relevant security experts, which may include existing governance bodies under the SEC or transitional governance to consider the impact of any exceptions.

4.3 Part 2 SRT Entry Criteria

The following entry criteria must be met by the DCC and Service Providers for Part 2a:

- Technical Readiness criteria associated with the commencement of SIT[5] must have been met;
- Solution Test Plan (inclusive of Part 2 SRT elements) approved by the DCC;
- Solution Test Specifications (inclusive of Part 2 SRT elements) prepared;
- Authority to Proceed Certificates must be issued by the DCC for the DSP, at least one CSP, the TSP and at least one RDP system;
- the SMKI test Service is available and ready to test (TSP Pre-Integration Testing successfully complete);
- Technical Readiness assessments complete with regards to the integration of the DSP's test SMKI Repository with the SMKI test Service[6];
- Requirements Traceability Matrix (DSP's and TSP's own RTMs per solution design), produced, which will be consolidated and extended to cover the scope of SRTA, per section 5.9, and approved by the DCC.

Additionally, the DCC will:

- select at least one protocol-certified[7] Communications Hub prototype from each CSP;
- select certified Devices where these are available, otherwise Part 2 SRT will commence with Devices that have been selected in accordance with relaxed criteria (following guidelines set out in the DSM) or Test Stubs. Should certified Devices or improved versions of Devices or Test Stubs become available they will be introduced in a controlled manner, per the requirements of Systems Integration Testing;

[5] In accordance with the SEC Panel Approved SIT Approach

[6] Per the Technical Readiness assessment of other systems as defined in the SIT Approach

[7] Per the requirements of the Systems Integration Testing

- select at least one set of certified Smart Metering Equipment for each fuel type, as selected via the Device Selection Methodology (or a DSP/CSP-approved Test Stub that is capable of processing SMKI Certificates, and utilising Public/Private Key pairs for end to end signing of messages, including the checking of Cryptographic Protection and confirming Validity steps).

Part 2a SRT will be undertaken using (to the extent reasonably practicable) actual Devices (rather than Test Stubs or other alternative arrangements).

In addition to the entry criteria above, the following entry criteria must be met by the DCC and Service Providers for Part 2b:

- SIT environment containing Devices containing a Root Certificate with an encrypted Apex Contingency public key for which:
    - the corresponding private key is available in the environment; and
    - the Symmetric encryption key is split into two parts; both parts are available in the test Recovery Environment.
- TSP establishes a new Root Key Pair, ready to issue a new Root Certificate Authority, and which includes the encrypted Apex Contingency Key generated as part of the test; and
- DSP has capability to generate CSRs for Recovery, ACB, TCoS and CSP Organisation Certificates available to create new Organisation Certificates ready for use within the Contingency Recovery processes tests.

4.4 Part 2 SRT Exit Criteria

The following exit criteria must be met by the DCC:

- exit criteria for Part 1 SRT met;
- 100% of planned tests run, or any exceptions documented and agreed with the DCC;
- at least 85% of planned tests passed, or any exceptions and impacts documented and agreed with the DCC;
- the level of defects is within the following thresholds per Service Provider, or any exceptions are documented and agreed with the DCC:
    - 0 Severity 1s (see Appendix A for Severity definitions)
    - 0 Severity 2s
    - 15 Severity 3s
    - 30 Severity 4s
    - 60 Severity 5s;
- the Test Completion Report has been issued in accordance with section 6.2;
- the appropriate Work-Off Plan has been produced and agreed by the DCC;

- all test results have been documented and evidence captured;
- a complete set of test issue logs produced;
- Relevant RTMs have been updated with test results, any new test cases, etc. upon exiting Part 2 SRT.

The DCC may take advice from relevant security experts, which may include existing governance bodies under the SEC or transitional governance to consider the impact of any exceptions.

4.5 Part 3 SRT Entry Criteria

The following entry criteria must be met by the DCC and Service Providers for Part 3 SRT:

- exit criteria for DSP Pre-Integration Testing successfully met for the required Change Requests, which deliver: Device Eligibility Checks; IKI File Signing solution; Recovery Environment; and Recovery Certificate Checks;
- exit criteria for TSP Pre-Integration Testing successfully met for the required Change Requests, which deliver: Device Eligibility Checks; and IKI File Signing solution;
- Solution Test Plan (inclusive of Part 3 SRT elements) approved by the DCC;
- Solution Test Specifications (inclusive of Part 3 SRT elements) prepared;
- the SMKI Recovery environment is available;
- Authority to Proceed Certificates must be issued by the DCC for Part 3 SRT.

4.6 Part 3 SRT Exit Criteria

The DCC will ensure that following exit criteria are met by the DCC and Service Providers for Part 3 SRT:

- 100% of planned tests run, or any exceptions documented and agreed with the DCC;
- at least 85% of planned tests passed, or any exceptions documented and agreed with the DCC;
- the level of defects is within the following thresholds per Service Provider, or any exceptions are documented and agreed with the DCC:
  - 0 Severity 1s (see Appendix A for Severity definitions)
  - 0 Severity 2s
  - 15 Severity 3s
  - 30 Severity 4s
  - 60 Severity 5s;

- the Test Completion Report has been issued in accordance with section 6.2;
- where appropriate, a Work-Off Plan has been produced and agreed by the DCC;
- all test results have been documented and evidence captured;
- a complete set of test issue logs produced

Details of Testing Issues outstanding and recorded on the Work-Off Plan that have the potential to impact Testing Participants undertaking SREPT will be made available to Testing Participants.

The DCC may take advice from relevant security experts, which may include existing governance bodies under the SEC or transitional governance to consider the impact of any exceptions.

4.7 SREPT Entry Criteria

SREPT using a DCC Gateway Connection cannot commence until the DCC has successfully completed Part 1a SRT, and SREPT using SMKI via the Internet Portal cannot commence until the DCC has successfully completed Part 1b SRT.

Each Party or RDP must successfully meet the entry criteria as defined in the SMKI & Repository Tests Scenarios Document (SRTSD) prior to commencing SREPT.

Details of Testing Issues outstanding and recorded on the Work-Off Plan that have the potential to impact Testing Participants undertaking SREPT will be made available to Testing Participants

Note: For the purposes of gaining Test Certificates Testing Participants should refer to the Enduring Testing Approach Document

Note: Testing Participants must comply with the Security Requirements set out in the Enduring Testing Approach Document.

4.8 SREPT Exit Criteria

The exit criteria that are set out in the SRTSD must be met.

4.9 SRT Exit Criteria

The following exit criteria must be met:

- Part 1 SRT Exit Criteria successfully achieved;
- Part 2 SRT Exit Criteria successfully achieved;
- Part 3 SRT Exit Criteria successfully achieved;
- at least one RDP has met the test success criteria for tests run, tests passed and testing issues as set out in the SIT Approach Document (section 6.6.3), which can only be achieved via their successful use of SMKI to sign registration data files;

- at least two Large Supplier Parties who are not an Affiliate of one another have each completed the SMKI and Repository Entry Process Tests[8] to become:
    - an Authorised Subscriber, and a Subscriber for Organisation and Device Certificates under the Test Certificate Policy[9];
    - eligible to access the SMKI Repository as set out in the SMKI RAPP

[8] This criterion will be updated to reflect any revision to the Parties mandated to complete SREPT as part of the exit criteria for SRT.

[9] This Test Certificate Policy is approved by Transition SMKI PMA Group (TPMAG), a working group set up by DECC and once approved will be published by the DCC.

5 Scope of Testing

5.1 Part 1 SRT Functional Testing

Part 1 SRT will validate:

- SMKI Registration Authority Policies and Procedures (SMKI RAPP) insofar as issuance of IKI credentials to the SMKI test Service and credentials to access the test SMKI Repository as set out in the SMKI RAPP;
- emergency suspension of SMKI Services:
    - suspend the provision of the SMKI Services;
    - suspend the rights of any SMKI Participant to receive (in whole or in part) the SMKI Services
- access control to ensure that only a party that is authorised can access the test SMKI Repository via the various interfaces;
- processing of Certificate Signing Requests and issuance of Test Certificates;
- lodging of Test Certificates to the test SMKI Repository;
- revocation of Test Organisation Certificate and IKI credentials;
- ability of the test SMKI Repository to be able to store and make available copies of artefacts as detailed in the SEC L5.1;
- access to the test SMKI Repository to view and/or obtain a copy of any document or information stored on it;
- the following interfaces provisioned for accessing the SMKI test Service;

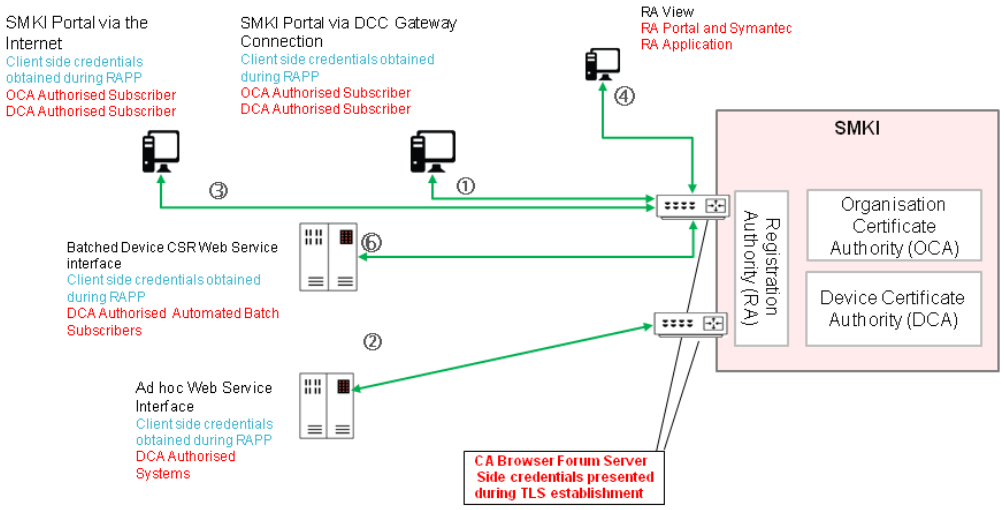


Figure 2 – SMKI Service Interface Overview

1. SMKI Portal interface via the DCC Gateway Connection
2. Web Service Interface that may be accessed by Parties' automated systems, and only accessible via the DCC Gateway Connection
3. SMKI Portal via the Internet made available over a secured Internet connection and accessed through a web browser that does not go through the DCC Gateway Connection
4. Portal Interface for SMKI Registration Authority Personnel
5. System-to-System interface between SMKI test Service and the test SMKI Repository
6. Batched Device CSR Web Service interface for the purposes of submitting batches of Device CSRs

- the following interfaces provisioned for accessing the test SMKI Repository;

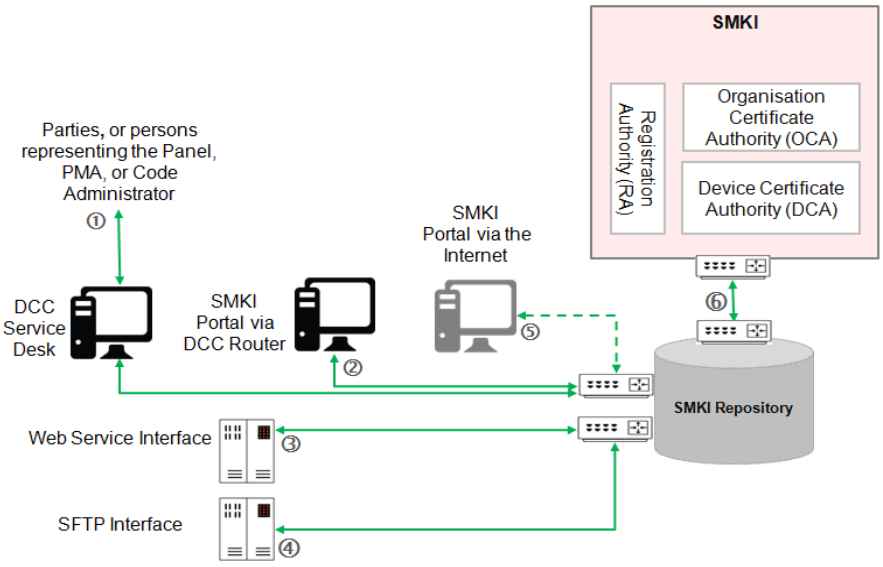


Figure 3 – SMKI Repository Interface Overview

1. Human Interface made available to Parties, or representatives of the SMKI PMA or Panel or Code Administrator via the DCC Service Desk or via (to be determined) a secure electronic channel
2. SMKI Portal interface accessed via a web browser and only accessible via the DCC Gateway Connection using username and password on the client and CA browser forum certificates on the server
3. System-to-System interface for the purposes of querying the test SMKI Repository using API key on the client and CA browser forum certificates on the server
4. SFTP interface for the purposes of obtaining copies of 'in use' Certificates from the test SMKI Repository using username and password
5. SMKI Portal via the Internet interface accessed via a web browser and accessible via an Internet connection secured using IKI Certificates (that does not go through the DCC Gateway Connection), for the purposes of obtaining a subset of Certificates necessary to support procurement of Devices. Also allows batch and ad hoc Device requests plus Organisation Certificate Requests, Repository requests, CRL Downloads, and .zip files containing anchor Certificates
6. System-to-system interface between SMKI test Service and the test SMKI Repository using IKI certificate on the DSP side and CA browser forum certificate on the TSP side

As noted in section 3.4, reliance is placed on tests that are performed in previous stages that are not impacted by the integration of solution components.

5.2 Part 2 SRT Functional Testing

Part 2a SRT functional testing will validate:

- the keys from within the test SMKI Repository that are required by the core components of the DCC solution in order to assure the chain of trust of the Organisation Certificates and use the correct public key to MAC messages being sent to meters[10];
- the test Certificates from within the test SMKI Repository that are required by the motorway in order to check Digital Signatures and confirm validity of test Certificates.

Test Scenarios are not defined in Section 11 to validate wider functional requirements as these will be achieved through PIT or SIT as part of sending the full suite of Service Requests.

Part 2b SRT functional testing will validate:

- the generation of the Apex Contingency Key pair by the DSP;
- generation of an Apex Contingency symmetric encryption key by the DSP;

10 Done whilst in the process of conducting Functional testing during SIT, sending the full suite of Service Requests to meters

- encryption of the Apex Contingency Public Key using the Apex Contingency Symmetric key by the DSP;
- splitting and secure storage of the Apex Contingency Symmetric encryption key;
- transfer of the encrypted Apex Contingency Public key to the TSP (the encrypted public key will be included in a new Root Certificate by the TSP for use in the following step[11]);
- execution of the processes to use the Apex Contingency key in a recovery scenario:
    - recombination of the Apex Contingency Symmetric encryption key;
    - activation of the ApexContingency private signing key;
    - replacement of the Root Certificate on devices in the SIT environment using updateSecurityCredentials command as set out in the GBCS:
        - in '`anyByContingency`' replacement mode;
        - signed by the ApexContingency private signing key;
        - containing the Symmetric Encryption Key.

5.3 Part 3 SRT Functional Testing

Part 3 SRT functional testing will validate:

- file signing for communications for the purposes of SMKI Recovery;
- the processes and procedures to enable:
    - recovery by a Subscriber using its Private Key to replace its Organisation Certificates on Devices;
    - recovery by the DCC using the Recovery Private Key to place DCC Access Control Broker Certificates on affected Devices;
    - recovery by the DCC using the Recovery Private Key to place new Supplier and Network Operator Organisation Certificates on Devices;
    - recovery from Compromise of the Apex Contingency Private Key or the Apex Contingency Symmetric Key;
    - recovery from Compromise of the Recovery Private Key; and
    - recovery from Compromise of the Issuing OCA Private Key.

[11] The TSP will also create a new Root key pair, establish a new Root CA, OCA and issue new Recovery, ACB, TCoS, Supplier and Network Operator Certificates to be used in the final step of this test. However, the creation of the new Root CA and Certificates falls outside the scope of Part 2b testing; it will already have been tested.

Each of these recovery scenarios will be defined within the SMKI Recovery Procedure SSD.

5.4 Part 1 SRT Non-Functional Testing

Part 1 SRT non-functional testing will validate:

- Target Response Times for:
    - SMKI test Service lodging of Certificates in the test SMKI Repository;
    - test SMKI Repository processing and making available Certificates, including batch requests (once received from SMKI test Service) over each interface, as shown in section 5.1;
    - request for a document over the test SMKI Repository Interfaces, as shown in section 5.1
- volume testing processing capability of the test SMKI Repository;
- volume/stress testing of the SMKI Service integrated with the test SMKI Repository subject to the constraints of the test environments used;
- Service Management systems required to support the SMKI Live Service

5.5 Part 2 SRT Non-Functional Testing

Part 2 SRT validates the integration of the SMKI and Repository Service within the wider DCC ecosystem and will be conducted within the SIT environment. SIT non-functional testing cannot be successfully passed without the concomitant level of non-functional performance and resilience of the SMKI and Repository Service. Therefore, no non-functional testing for Part 2 SRT is required. Non-functional testing will be further defined in Operational Acceptance Testing.

5.6 Part 3 SRT Non-Functional Testing

Part 3 SRT non-functional testing will validate:

- Target times for executing recovery procedures;
- Service Management systems required to support the IKI file signing solution and recovery.

5.7 SMKI Environment Commissioning

On completion of Part 1 SRT functional and non-functional testing, completion of testing of recovery functionality involving the Apex Contingency Key during Part 2b SRT and completion of SREPT by two Large Supplier Parties who are not an Affiliate of one another, the DCC, supported by the DSP and TSP, will commission the SMKI Live Service on the Production Environment.

SMKI Environment Commissioning will include:

- functionally regression testing the Production Build;
- disaster recovery testing of the SMKI Live Service;

- penetration testing;
- revalidating the Target Response Times for:
    - publishing ARLs and CRLs
    - response to a single Certificate Signing Request (both ad hoc and system to system interfaces);
    - response to a Batched Certificate Signing Request;
    - request for a document over the SMKI Repository Interface
- a volume/stress test of the SMKI Service integrated with the SMKI Repository, by issuing large numbers of Communications Hubs Certificates to a CSP

5.8 Quality Gates

Quality Gate Reviews are used to confirm that the Exit Criteria of the preceding Test Stage and the Entry Criteria of the upcoming Test Stage have been met.

The following table describes the Quality Gate Reviews for Part 1 SRT:

Quality Gate Review	Chair	Approver	Attendees
Between TSP PIT and Part 1 SRT	DSP	DSP	DCC, TSP
Between Part 1a SRT and SREPT	DSP	DCC	TSP
Prior to commencement of Part 1b	DSP	DSP	DCC, TSP
Between Part 1b SRT and SREPT	DSP	DCC	TSP
Prior to commencement of Part 2b	DSP	DSP	DCC, TSP
Prior to commencement of Part 3	DSP	DSP	DCC, TSP

The “Approver” of each Quality Gate Review Meeting will set the outcome as one of the following:

- preceding Test Stage can close, upcoming Test Stage can start, only minor (if any) remedial actions required;
- preceding Test Stage cannot close until remedial actions have been completed, upcoming Test Stage can start;
- preceding Test Stage can close, upcoming Test Stage cannot start until remedial actions have been completed;
- preceding Test Stage cannot close, upcoming Test Stage cannot start, until remedial actions have been completed

Each Quality Gate Review meeting will be a short, checklist-driven event at which previously assembled and validated evidence relating to the Exit and Entry Criteria is considered and decisions made to close the current Test Stage and start the next Test Stage. It is expected that Quality Gate Review meetings will be dry-run, including the provision of a draft of the Test Completion Report being issued 10 working days before the planned end of test execution, to enable issues to be

identified and resolved in a timely manner, and thereby avoid impacting the start date for any part of SRT.

The current Test Stage/Phase will complete (and achieve its Milestone) on attainment of its Exit Criteria. The next Stage/Phase will commence (and achieve its Milestone) on attainment of its Entry Criteria. The Quality Gate Review meeting will take place during the transition from the current to the next Test Stage.

To facilitate the operation of Quality Gate Reviews and the timely achievement of Test Stage Entry Criteria for any part of SRT, the DSP will publish weekly Test Readiness Reports for that part of SRT[12], as described in the Joint Test Strategy.

Additionally, two Quality Gate Reviews covering the commencement and completion of Part 2 SRT will be contained within the SMIP's Quality Gates 3 and 5 as described in the SIT Approach.

Any issues that have the potential to impact Testing Participants during SREPT will be notified through the Testing Issue Resolution Process.

5.9 Requirements Traceability

The DSP and TSP will each use their own tool to manage their requirements and demonstrate traceability to both the Solution Design (for the test SMKI Repository) and the Pre-Integration tests (for the SMKI test Service). The DSP and TSP will each provide the DCC with a Solution Design/PIT Requirements Traceability Matrix (RTM), extracted from these separate tools.

Prior to the start of SRT, the DSP will consolidate and extend these RTMs to include the relevant part of SRT tests and supply the results to the DCC.

[12] Part 2 SRT Test Readiness Reports will form part of the Test Readiness Reports for SIT

6 Test Reporting

6.1 Test Execution Reports

The DCC will provide the SEC Panel and the Secretary of State with a copy of the weekly Test Execution Reports for information, with details of any test issues anonymised and redacted as required, in accordance with Section H14 of the SEC.

Part 1a and Part 1b, Part 2b and Part 3 SRT reporting of test execution status will be via specific weekly Test Execution Reports.

Part 2a SRT reporting of test execution status will be contained within SIT weekly Test Execution Reports.The content of Test Execution Reports will, as a minimum, include:

- actual number of test scripts executed vs. planned, cumulative trend;
- actual number of test scripts passed vs. planned, cumulative trend;
- actual number of open and closed test issues vs. planned, cumulative trend;
- actual number of test issues outstanding, split by severity;
- progress against test exit criteria;
- top three Risks and Issues;
- overall RAG status

6.2 Test Completion Reports

At the end of Part 1, Part 2 and Part 3 SRT, the DSP will provide the DCC with a Test Completion Report. The DCC will provide this report to the Panel for information.

At the end of the Solution Test Stage, the DSP will provide the DCC with a Test Completion Report. Part 2 SRT Completion Report will be contained within that report. The DCC will provide this report to the Panel for information.

The DCC will gain assurance that the SRT exit criteria have been met through a range of activities, including monitoring execution of testing and resolution of testing issues, witnessing testing activities in line with Good Industry Practice, having consulted upon those activities in the SRT Approach Document (this document).

The DCC will, once the SRT exit criteria have been met in accordance with the SEC T5.19 and T5.20, and having consulted with the Parties who have participated, provide an SRT Completion Report to the SEC Panel.

Test Completion Reports provide the following information:

- Overview of testing undertaken
- Actual number of tests run, passed, failed, not run
- Explanation for any tests not run

- Test issue ids for failed tests
- Number of test issues outstanding, split by Severity
- Work off Plan for outstanding test issues
- Number and severity of test issues raised
- Specification of test environment used
- Recommendations for tests to be included in the next Test Stage.

The Test Completion Report for SRT will also include information regarding the completion of SMKI and Repository Entry Process Tests by two Large Supplier Parties.

7 Roles & Responsibilities

7.1 Test Team

The diagram below shows the structure of the Test Team.

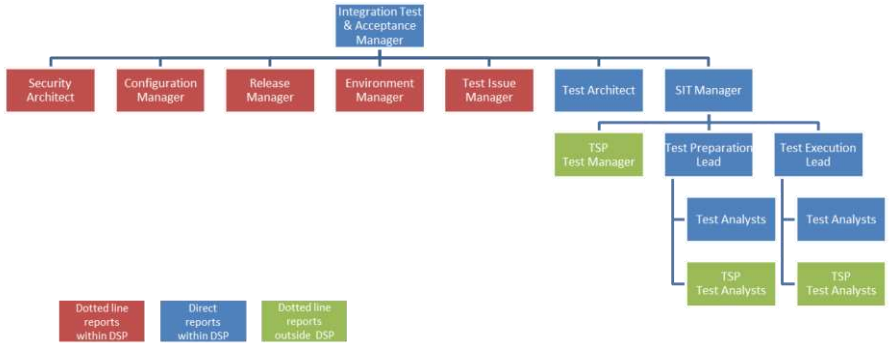


Figure 4 – Structure of Test Team

The roles in this structure are as follows:

- Integration Test and Acceptance Manager
  - responsible for all DSP Integration Test activities, including User Integration Testing
- TSP Test Manager
  - responsible for PIT testing of the SMKI Service
  - single point of contact for all design, development and technical queries on the SMKI Service
  - provides “local” management of preparation and execution for SRT tests within their agreed test boundary
- Security Architect
  - responsible for advising on all Security aspects of testing
- Configuration Manager
  - owns the master Configuration Plan which defines a) the Configuration Items (CIs) comprising the Smart Meter eco-system and b) the inter-dependencies between these CIs
  - responsible for configuration management of DSP CIs
- Release Manager
  - owns the master Release Schedule which shows a) when the various Releases are deployed to the test environments and b) the inter-dependencies between these releases

- responsible for releases of DSP solution elements

- Environment Manager
  - owns the master Environment Plan which shows a) the architecture of the various test environments and b) the communications links between these environments
  - responsible for the DSP test environment

- Test Issue Manager
  - responsible for chairing the Issue Resolution Board (IRB), expediting the resolution of outstanding test issues, agreeing which defect fixes go into which Releases, and reporting progress to stakeholders

- Test Architect
  - responsible for designing Integration test scenarios and test data, supporting Integration test Planning, designing and assuring Integration test procedures

- SIT Test Manager
  - responsible for planning and control of SIT (which is used for Part 2 SRT)

- Test Preparation Lead
  - responsible for designing and building test scripts

- Test Execution Lead
  - responsible for execution of test scripts

- Test Analysts
  - responsible for writing and executing test scripts
  - sourced from each SP, to work on tests within their agreed test boundary
  - numbers and profile to be determined

7.2 General

All parties involved in SRT shall:

- comply with the SEC and follow “Good Industry Practice” i.e. the exercise of that degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person engaged in a similar type of undertaking as that Party under the same or similar circumstances;

- take all reasonable steps to facilitate achievement of the SMKI and Repository Testing Objectives

7.3 DSP as Systems Integrator

In its role as Systems Integrator, the DSP will manage Part 1, Part 2 and Part 3 SRT and is responsible for the following activities:

- consolidate and extend RTMs to include the test for each part of SRT and supply the results to the DCC
- ensuring that activities for the part of SRT are carried out in line with the SRT Approach;
- overall planning and control of each part of SRT
- for tests within their agreed test boundary, under the direction of the Systems Integrator:
  - execute and monitor test scripts;
  - capture evidence;
  - report progress;
- for each part of SRT, maintaining Risk, Assumption, Issue and Dependency Logs;
- for each part of SRT, leading the design and creation of test scenarios, test scripts, test data and test environments;
- for each part of SRT, preparing test execution and environment usage schedules;
- for each part of SRT, supporting the TSP in their assigned test preparation and execution activities;
- for each part of SRT, managing test issue resolution, and supporting the TSP in the resolution process;
- for each part of SRT, producing the Requirements Traceability Matrices, Progress Reports and Test Completion Reports;
- for Quality Gate Reviews approving that Exit Criteria and Entry Criteria are met;
- support the DCC during Environment Commissioning

7.4 TSP

The TSP will:

- support the DSP as Systems Integrator in:
  - planning and control of each part of SRT;
  - design and creation of test scenarios, test scripts, test data and test environments;
  - preparing test execution and environment usage schedules;

- diagnosing test issues;
- producing Requirements Traceability Matrices, Progress Reports and Test Completion Reports

- establish, maintain and control their own test environments, in terms of software/hardware configuration and access control;
- for tests within their agreed test boundary, under the direction of the Systems Integrator:
  - execute and monitor test scripts;
  - capture evidence;
  - report progress;
- resolve test issues for their solution elements and undertaking PIT testing (including regression testing) of any fixes required; and
- support the DCC during SMKI Environment Commissioning

7.5 CSPs

Both CSP North and CSP Central/South will:

- for Part 2 and Part 3 SRT, support the DSP as Systems Integrator in:
  - planning and control
  - preparing test execution and environment usage schedules; and
  - diagnosing test issues
- for Part 2 and Part 3 SRT, establish, maintain and control their own test environments, in terms of software/hardware configuration and access control; and
- for Part 2 and Part 3 SRT, resolve test issues for their solution elements and undertaking PIT testing (including regression testing) of any fixes required

7.6 DCC Licensee

The DCC Licensee will:

- comply with its obligations under the approved SRT Approach (this document);
- ensure that the activities attributed to Service Providers that are described in this document are undertaken;
- use its reasonable endeavours to ensure that all of SMKI and Repository Testing is completed as soon as is reasonably practicable to do so;
- obtain sets of Devices from Device Manufacturers, as selected via the Device Selection Methodology for use in Part 2 and Part 3 SRT;

- support the DSP in the planning, control and operation of each part of SRT;
- assure each part of SRT planning, preparation and execution activities undertaken by the Systems Integrator and TSP;
- review and approve the relevant Test Documents, and issue the Authority to Proceed Certificates;
- participate in Quality Gate Reviews as described in Section 5.8;
- agree with the DSP and TSP a subset of the tests to be formally witnessed for each part of SRT;
- witness the execution of these tests at the end of each part of SRT;
- define and implement a process to audit the achievement of each part of SRT Testing Exit Criteria;
- control and manage SREPT, and provide support to Parties, including facilitation of concurrent testing of SEC Parties and the provision of analysts to achieve timely completion of SREPT[13]. To support this, SEC Parties are required to notify the DCC of their intention to participate in SREPT 60 working days prior to starting test; and
- manage SMKI Environment Commissioning

7.7 Testing Participants

Testing Participants will:

- conform to the SRTSD and this document with regards to planning, preparation, execution and completion of SREPT

[13] Further detail regarding DCC facilitating Parties undertaking and completing the SMKI and Repository Tests will be provided in the SMKI & Repository Test Scenarios Document.

8 Test Assurance / Audits

The DCC Test and Assurance team will carry out the following test assurance processes to audit and assure the testing carried out during each part of SRT.

8.1 Test Witnessing

The DCC Licensee will co-ordinate and witness an agreed amount of tests that are executed during each part of SRT. Part 2a SRT Test Witnessing will take place concurrent with SIT Test Witnessing. The aim of Test Witnessing is to gain assurance about the quality of the SMKI systems and verify the testing activities carried out by the DSP and TSP as the testing activities take place.

8.2 Product Inspections

By prior arrangement with the DSP and/or TSP on the timing, duration, scope and level, the DCC will be entitled to conduct on-site product inspections. The scope of these inspections will be:

- confirming that physical infrastructure meets design documents;
- confirming that necessary delivery notes for infrastructure exist;
- confirming that infrastructure is built appropriately;
- confirming that a process for assurance is followed;
- confirming that configuration of hardware, software and applications matches the design;
- confirming good industry practice is followed for asset tagging, cabling and racking;
- establishing that build scripts have been developed and tested; and
- confirming that relevant information is captured for configuration identification

The DCC will discuss the outcome of such Inspections with the DSP and/or TSP at the time of the inspection, and agree any actions arising (including completion dates) with the DSP and/or TSP.

9 Environments and Labs

The following table shows the names of the test environments that will be used for each part of SRT and SREPT.

Test Activity	DSP	TSP	CSP N	CSP C/S
Part 1a SRT	UIT	UIT	N/A	N/A
Part 1b SRT	SIT	SIT	N/A	N/A
Part 2a SRT	SIT	SIT	SIT	SIT
Part 2b SRT	SIT	SIT	SIT	SIT
Part 3	SIT	SIT	SIT	SIT
SREPT	UIT	UIT	N/A	N/A

Table 1 - Test Environments

The TSP and each CSP are responsible for establishing, maintaining and controlling their own Test Environments.

9.1 Test Labs

Each CSP will provide a Test Lab which will house:

- Smart Meters (or a DSP/CSP-approved Test Stub that is capable of processing SMKI Certificates, and utilising Public/Private Key pairs for end to end decryption and encryption of messages),
- Certified Communications Hubs; and
- Smart Metering equipment for use during Part 2 and Part 3 SRT, selected in accordance with the Device Selection Methodology.

Note, these requirements are required to facilitate Part 2b and Part 3 SRT, including the Recovery Procedures, which is conducted in the SIT environment.

10 Test Issue Management

10.1 Logging and triage of Test Issues

During each part of SRT and SREPT, all test issues will be logged in HP ALM by the person executing the test. New test issues will be reviewed at least daily by the relevant DSP/TSP/CSP Test Manager, who will:

- classify them as one of:
  - testing issue:
    - that prevents execution of a test; or
    - that causes an unexplained or unexpected outcome or response to a test
  - not a testing issue (e.g. a misunderstanding);
  - duplicate;
  - change; or
  - need more information;
- set the severity and priority (see Appendix A for definitions);
- assign the test issue to the relevant resolver group. Should this lie outside the DSP, TSP, or relevant CSP organisation, the test issue will be assigned to the DSP Test Issue Manager

10.2 Resolution of Test Issues

The DSP Test Issue Manager will:

- regularly review all outstanding test issues to ensure that they are resolved at the requisite speed;
- involve the TSP and or relevant CSP as required in the triage and resolution of issues;
- agree with the relevant DSP/TSP/CSP Test Managers the defect fixes to be included in each Release to the Test1 or Test2 environments;
- report progress directly to stakeholders

The proposed target response times are those set out in the Joint Test Strategy.

10.2.1 Assurance

The Issue Review Board (IRB), comprising of the DSP's, TSP's, each of the CSPs' Design Authority, the DCC, and DECC and chaired by the DSP Test Issue Manager, will meet daily (and on demand for urgent test issues which are delaying testing) to:

- resolve cases where the ownership of a test issue is disputed;

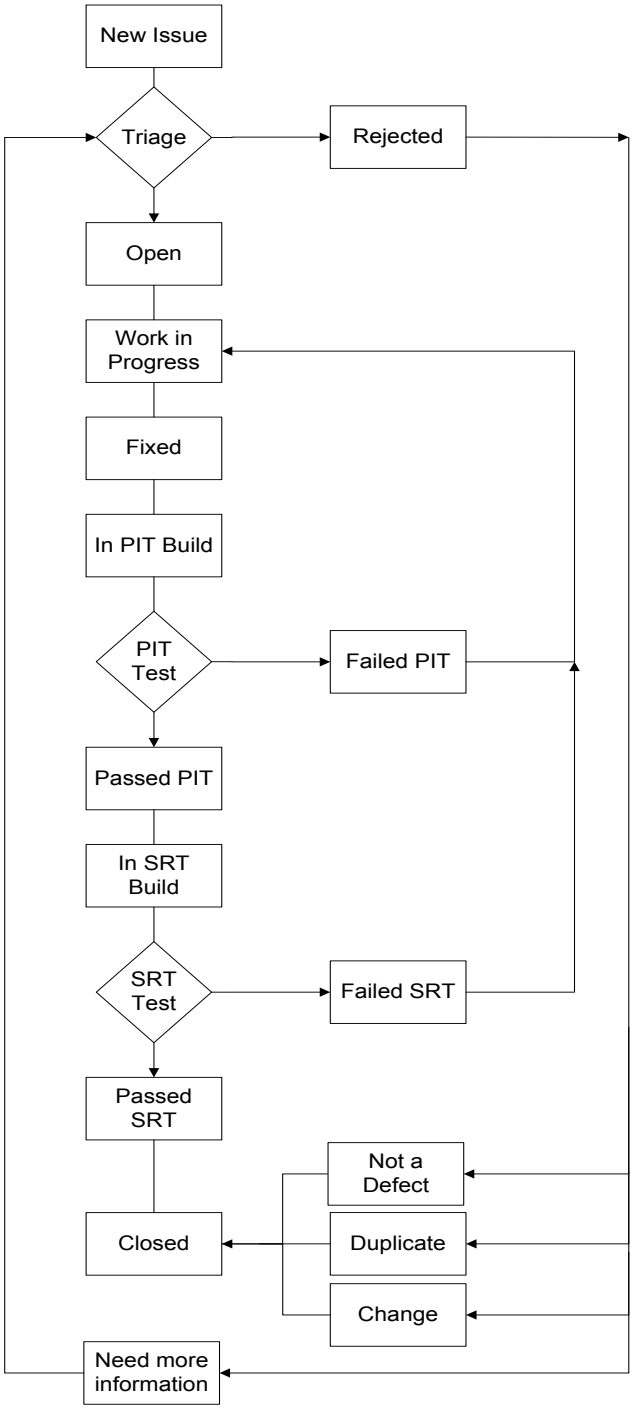
- confirm, by a process of sampling, that test issues are being given the correct Severity by the local triage process; and
- confirm, by a process of sampling, that Priority 1 and 2 defects are being resolved at the requisite speed

10.3 Reporting of Test Issues

Information on the status of test issues will be reported by the DSP to the DCC in the weekly Test Execution reports described in the Joint Test Strategy.

10.4 Test Issue Management Process

The high level lifecycle for test issues raised during Part 1 and Part 2 SRT is shown in the following diagram.



Note that test issues can be passed back to “Triage” from the various process steps (e.g. “Failed PIT”), but these links are not shown on the diagram in order to preserve clarity. Test Issues which are agreed to be a Change will follow the DCC Change Control process (set out in the “Core SP Change Management Process” document).

11 SMKI & Repository Test Scenarios

The following Test Scenarios have been identified for each part of SRT. Further details of the test scenarios will be set out in the Test Specification provided for each part of SRT[14].

The test scenarios defined within each subsection below will be executed in the following SRT stages:

Stage	Subsections
1a	11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.7, 11.8
1b	11.9
2a	11.10 (and SIT testing of Service Requests, not shown)
2b	11.11
3	11.12, 11.13

A pre-requisite to performing these scenarios is that the Enduring Testing Approach is followed (such that credentials for AROs to access Test SMKI Services and Test SMKI Repository Services can be provided).

11.1 Security Credentials Access Tests to SMKI

ID	SMKI 02
Title:	**Using individual security credentials to access to the SMKI Service, through the SMKI Portal Interface via the DCC Gateway Connection, using the security credentials supplied by the DCC.**
Description	• **To prove that the SafeNet Client[15] Installed on ARO's computer validates their access details (and that the SafeNet Client can be downloaded if accessing for the first time via the client)** • **To prove that a Party authorised representative can use the FIPS token which is registered to them and their organisation when accessing the SMKI Portal Interface via the DCC Gateway Connection**

ID	SMKI 03
Title:	**Using security credentials to access the SMKI Service, through the SMKI Web Service Interface, and the Batched Device CSR Web Service Interface, using the security credentials supplied by the DCC.**
Description	• **To prove that the Organisation can access the SMKI Service through the SMKI Web Service Interfaces using the IKI Credentials** • **To prove IKI credentials are correct to authenticate the SMKI Web Service Interfaces.**

[14] A 'Party' as referenced in the Test Scenarios is a Test User created by the DCC for the purposes of SRT

[15] The DCC makes available to PKI Client software (SafeNet Client), as set out in section 2.3.1 of the SMKI Code of Connection.

11.2 Security Credentials Access Tests to the test SMKI Repository

ID	SMKI 05
Title:	Using individual security credentials to access test SMKI Repository using the SMKI Repository Portal Interface via the DCC Gateway Connection.
Description	• To prove access the test SMKI Repository using the SMKI Portal Interface via the DCC Gateway connection using the SMKI URL, log in details and password.

ID	SMKI 06
Title:	Using security credentials to access the test SMKI Repository using the SMKI Repository Web Service Interface.
Description	• To prove that an Organisation's ARO can access the test SMKI Repository using the SMKI Repository Web Service Interface using the issued SMKI API connection and valid API Key.

ID	SMKI 07
Title:	Using security credentials to access the test SMKI Repository using the SMKI Repository SFTP (Secure File Transfer Protocol) Interface.
Description	• To prove that an Organisation's ARO can access the test SMKI Repository using the SMKI Repository SFTP (Secure File Transfer Protocol) Interface using the issued username and password.

ID	SMKI 38
Title:	Download Zip files of Anchor Slot Certificates via the Portal
Description	• To prove Zip files of anchor slot Certificates can be downloaded

ID	SMKI 48
Title:	Accessing the CRL using the test SMKI Repository Portal Interface via the DCC Gateway Connection
Description	• To prove that a Party's ARO can access the CRL using the SMKI Portal Interface via the DCC Gateway Connection

ID	SMKI 49

Title:	**Download copies of the SMKI Repository using the Secure File Transfer Protocol (SFTP)**
Description	• **To prove that a Party's ARO can download a copy of the SMKI Repository in-use Certificates using the SFTP (Secure File Transfer Protocol)** • **To prove that a Party's ARO can download a copy of the daily delta SMKI Repository in-use Certificates using the SFTP (Secure File Transfer Protocol)**

ID	SMKI 50
Title:	**Access the CRL using the test SMKI Repository Web Service Interface**
Description	• **To prove that a Party's ARO can access the CRL using the SMKI Repository Web Service Interface**

11.3 Management of Security (Authentication) Credentials

ID	SMKI 09
Title:	**Update (change PIN or decommission) of an ARO and/or AROs security credentials to access the SMKI Repository. This test also includes the adding of a new ARO after a Party has been registered with the DCC.**
Description	• **To prove that a Party can change their PIN or decommission their security credentials to access the SMKI.** • **To prove that addition AROs may be added to acquire access to SMKI.**

ID	SMKI 16
Title:	**Remove a user from accessing SMKI and the test SMKI Repository.**
Description	• **To prove that a Party's access to the SMKI and test SMKI Repository can be removed**

ID	SMKI 18
Title:	**Manage login details and contact information for the test SMKI Repository Portal Interface (DCC Gateway Users) using the profile page**
Description	• **To prove that the Portal Interface user name and password can be updated** • **To prove that contact information can be updated**

ID	SMKI 19

Title:	**Reconfigure API connection to regenerate API key through the test SMKI Repository Portal Interface**
Description	• **To prove that a party is able to regenerate their API Key and continue to use the Web Service Interface**

ID	SMKI 20
Title:	**Manage login details for access to the SFTP Server on the test SMKI Repository Portal Interface**
Description	• **To prove that a party is able to change their SFTP password within the user profile section of the test SMKI Repository Portal**

11.4 Submission of Certificate Signing Requests

ID	SMKI 22
Title:	**Submit Organisation Certificate Signing Requests (CSR) and receive Organisation Certificates using the Portal Interface via DCC Gateway Connection.**
Description	• **To prove a Party is capable of generating an asymmetric key pair and submit a Certificate Signing Request in the correct Format as detailed in the SMKI Interface Design Specification.** • **To prove that Certificate Signing Requests are in the correct format with true and accurate information** • **To prove users can resubmit further CSRs following rejection by the DCC** • **To prove Parties can download their Certificates, to confirm the information contained in the resulting Certificate is consistent with the information contained within the corresponding CSR** • **To prove that Certificate can be rejected** • **The Same Organisation Certificate may be retrieved from the test SMKI Repository** • **To prove that Certificates can be downloaded** • **To prove that the Organisation Certificate may be retrieved from the test SMKI Repository**

ID	SMKI 23
Title:	**Submit an Ad Hoc Certificate Signing Request (CSR) and receive Certificates for Devices through the Portal Interface via DCC Gateway Connection.**
Description	• **To prove that a Certificate Signing Request derived from a Device asymmetric key pair in the correct Format can be submitted as detailed in the SMKI Interface Design Specification.** • **To Prove that Certificate Signing Requests are in the correct format with accurate information** • **To prove that they can resubmit further CSRs following rejection by the DCC** • **To prove that Parties can download individual Device Certificates, to**

	confirm the information contained in the resulting Certificate is consistent with the information contained within the corresponding CSR • To prove that the Device Certificate is also lodged in the test SMKI Repository

ID	SMKI 24
Title:	Submit Batch Certificate Signing Request (CSR) and receive Certificates for Devices through the Portal Interface via DCC Gateway Connection.
Description	• To prove that a Certificate Signing Request derived from a Device asymmetric key pair in the correct Format can be submitted as detailed in the SMKI Interface Design Specification. • To Prove that Certificate signing requests are in the correct format with accurate information • To prove that they can resubmit further CSRs following rejection by the DCC • To prove that Parties can download their Device Certificates in zipped batches, to confirm the information contained in the resulting Certificate is consistent with the information contained within the corresponding CSR • To prove that a Device Certificate is also lodged in the test SMKI Repository

ID	SMKI 25
Title:	Submit an Individual Device Certificate Signing Request (CSR) and receive Certificates for Devices via the Web Service Interface.
Description	• To prove that a Certificate Signing Request derived from a Device asymmetric key pair in the correct Format can be submitted as detailed in the SMKI Interface Design Specification. • To Prove that Certificate Signing Requests are in the correct format with accurate information • To prove that they can resubmit further CSRs following rejection by the DCC • To prove that Parties can retrieve Device Certificates from the synchronous web service response, to confirm the information contained in the resulting Certificate is consistent with the information contained within the corresponding CSR • To prove that a Certificate can be rejected • To prove that a Device Certificate is also lodged in the test SMKI Repository

ID	SMKI 57
Title:	Submit a Batched Device Certificate Signing Request (CSR) and receive Certificates for Devices via the Web Service Interface.
Description	• To prove that a Certificate Signing Request derived from a Device asymmetric key pair in the correct Format can be submitted as detailed in the SMKI Interface Design Specification • To Prove that Certificate Signing Requests are in the correct format with accurate information • To prove that they can resubmit further CSRs following rejection by the DCC • To prove that Parties can download their Device Certificates in batches, to confirm the information contained in the resulting Certificate is consistent with the information contained within the corresponding CSR • To prove that a Device Certificate is also lodged in the test SMKI Repository

11.5 Collection of Documents & Information from the test SMKI Repository

ID	SMKI 29
Title:	Download a copy of all in use Test SMKI Certificates from the test SMKI Repository via SFTP (Secure File Transfer Protocol) Interface.
Description	• To prove a complete copy of all 'In Use' Certificates (including OCA and DCA issued Certificates can be downloaded).

ID	SMKI 30
Title:	Download a daily Delta of Test SMKI Certificates from the test SMKI Repository via SFTP Interface.
Description	• To prove a partial/'Daily Delta File' batch containing 'In Use' Certificates published to the test SMKI Repository during the preceding twenty four hours can be downloaded up to seven days from publication

11.6 Query the test SMKI Repository and Retrieve Documents & Information

ID	SMKI 31
Title:	Interrogate the test SMKI Repository via the Portal Interface via the DCC Gateway Connection in order to prove that an Organisation Certificate is now contained in the test SMKI Repository and can be retrieved.
Description	• To prove a Party is able to query the test SMKI Repository using selection criteria to determine the location of their Certificate in the test SMKI Repository • To prove a Party is able to download the located Certificate

ID	SMKI 32
Title:	Query the test SMKI Repository via the Web Services Interface in order to prove that an Organisation Certificate is now contained within the test SMKI Repository and can be retrieved.
Description	• To prove a Party is able to query the test SMKI Repository using selection criteria to determine the location of their Certificate in the test SMKI Repository • To prove a Party is able to download the located Certificate

ID	SMKI 33
Title:	Query via the Portal Interface via DCC Gateway Connection whether a Device's public key Certificate is in the test SMKI Repository
Description	• To prove a Party is able to query the test SMKI Repository using selection criteria to determine the location of the Device Certificate in the test SMKI Repository • To prove a Party is able to download the located Certificate

ID	SMKI 34
Title:	Query via the Web Service Interface whether a Device's public key Certificate is in the test SMKI Repository and that they can retrieve it
Description	• To prove a Party is able to query the test SMKI Repository using selection criteria to determine the location of the Device Certificate in the test SMKI Repository • To prove a Party is able to download the located Certificate

11.7 Ad Hoc Web Services Interface

ID	SMKI 61
Title:	Test the Ad Hoc Web Services Interface
Description	• To prove that a Party can send via the Web Services Interface a Device Certificate Signing Request for a Device[16] that has already been issued with a Certificate. • To prove that necessary checks are applied by the DCC (i.e. that a Certificate has been previously issued for the Device) • To prove a Certificate for this Device is returned from the DCA to the Party. DCC also lodge the Certificate in the test SMKI Repository.

[16] Actual Devices will not be used during Part 1 SRT and this scenario will be performed using Test Certificates.

11.8 Submission of a Revocation Request

ID	SMKI 42
Title:	Revocation of an IKI Certificate
Description	• To prove that the revocation process can be followed and IKI credentials are revoked • To prove that following revocation, new IKI credentials can be used successfully and that the revoked Certificate can no longer be used

ID	SMKI 43
Title:	Revocation of an Organisation Certificate
Description	• To prove that an Organisation Certificate can be revoked • To prove that following revocation, a new Organisation Certificate can be requested • To prove that the revoked Certificate appears on the next Certificate Revocation List (CRL).

11.9 SMKI via the Internet Portal

ID	SMKI 04
Title:	Using individual security credentials to access to the SMKI Service, through the SMKI Portal Interface via the Internet, using the security credentials supplied by the DCC.
Description	• To prove that the SafeNet Client Installed on ARO's computer validates their access details • To prove that a Party authorised representative can use the FIPS token which is registered to them and their organisation when accessing the SMKI Portal Interface via the Internet

ID	SMKI 08
Title:	Access the Organisation CRL, ARL & Certificate Bundles using the test SMKI Portal Interface via the Internet
Description	• To prove that a Party's ARO can access the CRL, ARL & Certificate Bundles using the SMKI Portal Interface via the Internet

ID	SMKI 26
Title:	Submit Organisational Certificate Signing Request (CSR) using the Portal Interface
Description	• To Prove that Certificate Signing Requests are in the correct format with true and accurate information • To prove that Non DCC Gateway users can download their Organisational Certificates

ID	SMKI 27
Title:	Submit Device Certificate Signing Request (CSR) via the SMKI Portal Interface via the Internet
Description	• To prove a Non-Gateway user is capable of submitting a Certificate Signing Request in the correct format as detailed in the SMKI Interface Design Specification • To Prove that Certificate Signing Requests are in the correct format with true and accurate information • To prove that a Non-Gateway User can download their Device Certificates, to confirm the information contained in the resulting Certificate is consistent with the information contained within the corresponding CSR

ID	SMKI 28
Title:	Submit a Batch Device Certificate Signing Request (CSR) via the Portal Interface via the Internet
Description	• To prove a Non-Gateway user is capable of generating a Device asymmetric key pair and submit a Certificate Signing Request in the correct format as detailed in the SMKI Interface Design Specification • To Prove that Certificate Signing Requests are in the correct format with true and accurate information • To prove that a Non-Gateway User can resubmit further CSRs following rejection by the DCC • To prove that a Non-Gateway User can download their Device Certificates in zipped batches, to confirm the information contained in the resulting Certificates is consistent with the information contained within the corresponding CSRs • To prove that a Non-Gateway user can reject a Certificate

11.10 Emergency Suspension

ID	SMKI 60
Title:	Emergency Suspension of SMKI Services
Description	• To prove that the SMKI Services and/or any other Services which rely on the use of Certificates can be suspended.

11.11 Recovery - Apex Contingency Key

ID	SMKI 53
Title:	Recovery from Compromise of Contingency Private Symmetric Key following the process outlined in the SMKI Recovery Procedure.
Description	• To prove that a new Contingency Symmetric Key Pair can be generated by the Key Custodian • To prove that a new wrapped Apex Contingency Key can be generated • To prove that a new Root OCA Key Pair / Certificate (signed with old

	/ new root) can be generated • To prove that a new Issuing OCA Key Pair / Certificate can be generated • To prove that old Root / Issuing OCA Certificates cannot be used to sign new Certificates • To prove that new Root / Issuing OCA Certificates can be lodged in the SMKI Repository • To Prove that Replacement of Root OCA Certificates can be monitored • To prove that replaced Contingency Private Keys / Certificates can be destroyed.

11.12 File Signing

ID	SMKI 58
Title:	Process a file signed using IKI RSA Token
Description	• To prove that a Party can create and submit a file using IKI RSA token • To prove that the DCC can authenticate the signed file • To prove that the signed file can be correctly processed using the relevant Certificate

ID	SMKI 59
Title:	Process a file signed using SMKI Private Key associated with an Organisation Certificate
Description	• To prove that a Party or RDP (or the DCC) can create and submit a file using SMKI Private Key associated with an Organisation Certificate • To prove that the DCC (or a Party or RDP) can authenticate the signed file • To prove that the signed file can be correctly processed using the relevant Certificate

11.13 Recovery – Other than Apex Contingency Key

These test scenarios have been removed from this document and will be further defined in the SMK I Recovery Procedure SEC Subsidiary Document.

Appendix A

Test Issue Severities

The following table lists the standard Test Issue Severities[17]:

Issue Severity	Description
1	An Issue which: • prevents a DCC Service User or large group of DCC Service Users from using the DCC Service User Systems and/or any DCC Services; • has a critical adverse impact on the activities of the DCC; • could cause significant financial loss and/or disruption to the DCC services or DCC Service Users[18]; or • Results in any material loss or corruption of Data. Non-exhaustive examples: • An Issue leading to Non-availability of the DCC Data Services; • An Issue leading to Non-availability of the CSP Core solution element(s).
2	An Issue which: • has a major (but not critical) adverse impact on the activities of the DCC but the service is still working at a reduced capacity; or • causes limited financial loss and/or disruption to the DCC Non-exhaustive examples: • An Issue leading to Non-availability of the Network Management Centre; • An Issue leading to loss of resilience of the SMWAN Gateway; • Large areas of functionality will not be able to be tested.
3	An Issue which: • has a major adverse impact on the activities of the DCC but which can be reduced to a moderate adverse impact through a work around; or • has a moderate adverse impact on the activities of the DCC.
4	An Issue which: • has a minor adverse impact on the activities of the DCC. Non-exhaustive examples: • Minor service interruptions in the business process or functionality of the DCC Systems and / or service.
5	An Issue which: • has minimal impact to the activities of the DCC. Non-exhaustive examples • Trivial issues with workarounds which are noted for future releases but minimal impact of running existing services.

[17] This table describing Test Issue Severities is taken from the Testing and Acceptance schedule of the Service Provider contracts. References to 'Service User' should be read as 'Testing Participant' in this context.

[18] For the purposes of SMKI & Repository Testing disruption should be considered to include security compromises.

Test Issue Priorities

The following table lists the standard Test Issue Priorities:

Testing Issue Priority	Description
1	All test progress is blocked by the testing issue.
2	Testing not completely blocked by the testing issue but the impact on test progress is significant.
3	Testing can proceed but the work-around for the testing issue has moderate impact on test progress.
4	Testing can proceed and the testing issue has little/no impact on test progress.